**CONGRESSO NACIONAL**
**COMISSÃO MISTA DE PLANOS, ORÇAMENTOS E FISCALIZAÇÃO**
**SISTEMA DE ELABORAÇÃO DE EMENDAS ÀS LEIS ORÇAMENTÁRIAS**
**PLN 0020 / 2017 - LOA**

Data: 17/10/2017
Hora: 15:18


# ESPELHO DE EMENDA DE APROPRIAÇÃO DE DESPESA

EMENTA
Exército Brasileiro – Implantação do Sistema de Defesa Cibernética

MODALIDADE DA EMENDA
Comissão

TIPO DE EMENDA
Aprop.- Acréscimo

LOCALIDADE BENEFICIADA
9000000 - Nacional

COMPLEMENTO DA LOCALIDADE

ESFERA ORÇAMENTÁRIA
Orçamento Fiscal

UNIDADE ORÇAMENTÁRIA PRETENDIDA
Comando do Exército

FUNCIONAL / AÇÃO / SUBTÍTULO
05.126.2058.147F.0001
Implantação de Sistema de Defesa Cibernética para a Defesa Nacional
Nacional

ESPECIFICAÇÃO DA META
Sistema implantado(% de execução física)

QUANTIDADE
6

ACRÉSCIMOS À PROGRAMAÇÃO (EM R$ 1,00)

| GND | | MOD. APLICAÇÃO | | RP | Valor Acrescido |
|---|---|---|---|---|---|
| 4 | Investimentos | 90 | Aplic. Diretas | 2 | 70.000.000 |
| | | | TOTAL ..... | | 70.000.000 |

CANCELAMENTOS COMPENSATÓRIOS

| SEQUENCIAL | FONTE | GND | | MOD. APLICAÇÃO | | ID | RP | Valor Deduzido |
|---|---|---|---|---|---|---|---|---|
| 003012 | 100 | 9 | Reserva de Contingência | 99 | A Definir | 0 | 2 | 70.000.000 |
| | | | | | TOTAL ..... | | | 70.000.000 |

JUSTIFICATIVA

No processo natural de globalização que vive atualmente a humanidade, a tecnologia da informação tem tido um papel preponderante. A proximidade e as facilidades que ela oferece têm permitido um crescimento humano e social em todos os sentidos, inclusive no campo da defesa e da segurança. Entretanto, a Sociedade da Informação encontra-se refém da tecnologia impondo à defesa e à proteção da informação, cada vez mais, tratamento cuidadoso e organizado por parte dos Estados.
A descoberta de falhas e vulnerabilidades nos diversos processos que envolvem a segurança de TI tem permitido o surgimento e o crescimento do chamado cybercrime (crime cibernético). Como evolução natural, está em evidência uma nova modalidade de guerra assimétrica, a cyberwar (guerra cibernética). Nela são atacados os centros dos Poderes civis e militares e ainda os principais centros de comunicação e controle dos serviços críticos, como sistemas de comunicações, saúde pública, energia e outros.
Em face de seu grau de desenvolvimento e projeção internacional, a infraestrutura do Brasil está calcada em sistemas de TI suscetíveis a inúmeras agressões cibernéticas provenientes de governos estrangeiros, instituições, organizações criminosas ou mesmo de grupos terroristas, o ciberterrorismo. O terrorismo cibernético pode aplicar os princípios da Guerra Psicológica atuando de forma dissimulada através da divulgação de notícias falsas e boatos, que se difundem rapidamente, ou mesmo de levar o País a uma situação de paralisia estratégica.
Em virtude das ameaças cibernéticas mencionadas a que está sujeito e em conformidade com a Estratégia Nacional de Defesa, o Brasil deve buscar autonomia nas tecnologias cibernéticas estabelecendo parcerias estratégicas por meio da aquisição de equipamentos e do fomento à pesquisa e ao desenvolvimento de sistemas de defesa cibernéticos nacionais. As iniciativas cibernéticas no campo da defesa estarão alinhadas com as diretrizes estratégicas do governo para a capacitação nos campos industrial e militar que estabelecerão regras e procedimentos para o uso de táticas de defesa cibernética.
As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, prioritariamente, as tecnologias de comunicação entre as Forças Armadas de modo a assegurar sua capacidade para atuar em rede e contemplarão o poder de comunicação satelital entre as forças singulares.



AUTOR DA EMENDA
5011 - Com. Ciencia,Tecn. Com. Informatica